FortiExtender Cloud Handbook

VERSION 1.0.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.comMa

May 1, 2018

FortiExtender Cloud 1.0.0 Handbook

1st Edition

TABLE OF CONTENTS

Change log

Date	Change Description
05/01/2018	FortiExtender Cloud v1.0.0 handbook initial release.

Introduction

Welcome, and thank you for choosing FortiExtender Cloud.

FortiExtender Cloud enables ultra fast deployment and simplified management of the FortiExtender equipped networks spread across various geographic locations. FortiExtender cloud has been designed with an intuitive single pane of glass management interface and workflow to reduce complexity, increase visibility and actionable insights. This combination allows for faster remote site bring-up with ease of troubleshooting leading to reduced total cost of ownership.

Supported devices

FortiExtender Cloud supports FortiExtender devices with the following models and versions:

Device Model	Device Version
FEXT-40D-AMEU	v3.3 build number 431

NOTE: FortiExtender build number 431 can only be managed from the cloud and not from the FortiGate.

Licensing

FortiExtender Cloud provides full functionality, free of charge, for **ten** FortiExtender devices. You must purchase a license before you can add additional devices.

Contact your primary Fortinet Service Provider for more information.

Getting started

Accessing FortiExtender Cloud

To access FortiExtender Cloud, you can either create a new Fortinet Customer Service and Support account, or use an existing FortiGate account.

Go to https://fortiextender.forticloud.com and follow the steps to sign up or log in.

After you sign in with FortiCare, you will be redirected to the FortiExtender Cloud portal.

Next Steps

Configuring FortiExtender devices—Deploy your FortiExtender devices using Zero Touch Provisioning. See "Zero Touch Provisioning" on page 7 for more information.

Monitoring FortiExtender devices—Central monitoring gives an overview of all the devices in the cloud, while device management lets you examine and remotely operate individual devices. See "Central monitoring" on page 9 or "Device management" on page 10 for more information.

Grouping FortiExtender devices—Put your devices into groups to help keep them organized. See "Grouping" on page 13 for more information.

Adding users—FortiExtender Cloud supports Role Based Access Control. See "Role Based Access Control" on page 15 for more information.

API—FortiExtender Cloud allows for API access. See "API" on page 16 for more information.

Zero Touch Provisioning

FortiExtender Cloud features Zero Touch Provisioning, which involves importing devices into the cloud, creating device templates, and automatically applying the necessary configuration and firmware on the devices.

Importing devices into the cloud

Import devices into FortiExtender Cloud by using the device's cloud key.

NOTE: The cloud key is provided by Fortinet. It maps to the corresponding device's Serial Number. If your device does not have a cloud key, contact Fortinet Service and Support.

1. From the Home page, click **ADD DEVICE**.
   A dialog box will pop up.
2. Input the device's Cloud Key, then click **ADD**.
   The new device will be added to the tasklist as an "In Stock" device.

NOTE: You can also add devices from the Inventory page.

Creating a device template

A device template is required to deploy devices from the cloud. Click **Device Template** to go to the device template page.

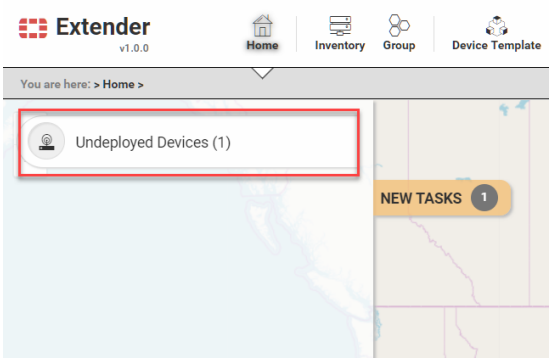
NOTE: You can add pre-defined configuration profiles and plans to device templates. Click **Config** or **Plan** to go to the corresponding page.

Deploying devices

All devices fall into one of three categories:

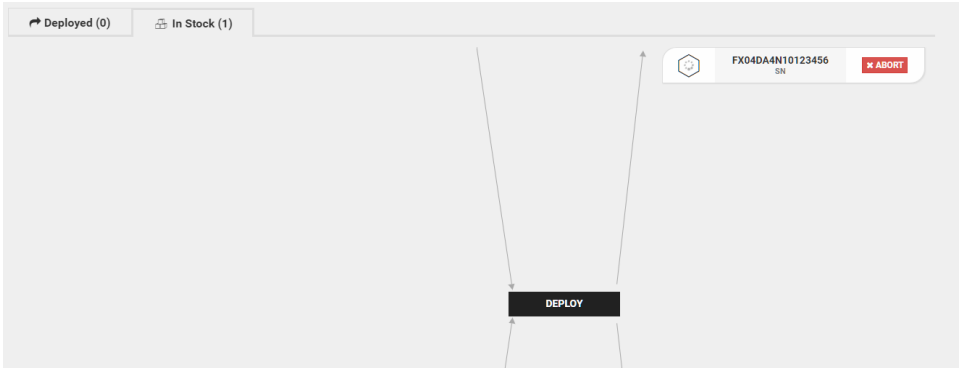
- In Stock—The device is imported, but not deployed.
- Deploying—The device has been deployed and is waiting to be physically installed.
- Deployed—The device is fully installed and online, synced with configured firmware and configurations.

1. Click on the Undeployed Devices task from the task list.



A list of all undeployed devices will be shown.

2. Select an undeployed device and click **DEPLOY**.
3. Select a device template.
4. Click **Apply**.
   The device will change to the "Deploying" state. It is now ready for on-site installation.



Synchronizing devices

Connect the device to the internet via the LAN ethernet port. The device will automatically synchronize firmware, configurations, and dataplans using internet connectivity over wired ethernet.

Once the device is synced, it can then be moved physically to an intended physical location.

Alternatively, if a LAN port is not available, configure the Carrier and APN settings on the device, insert the SIM card, and the device will automatically synchronize.

Upgrading firmware

Select a configuration and change the OS firmware or modem firmware. Devices currently using this configuration will be upgraded automatically.

Open the device event line to monitor the results.

Undeploying devices

1. Click on **Inventory**, located at the top.
2. Select a device, then click **UNDEPLOY**.

Central monitoring

FortiExtender Cloud features Central monitoring, which provides an overview of all the devices in real time. Central monitoring is accessible by clicking the **Monitor** button, located at the top of the screen.

Monitoring panels

Global eventline—This shows events that occurred in the past 24 hours.

Usage by device—This shows the top ten devices that use the most data, along with the amount of data used.

Usage by group—This shows the amount of data used by each group of devices.

Usage by plan—This shows the amount of data used per plan.

Unstable devices—This shows the top ten most unstable devices. A device is unstable if it frequently experiences disconnects, experiences a weak signal, alternates between LTE and 3G/4G, has poor bandwidth, or is offline for a long period of time.

Usage by carrier—This shows the amount of data used per carrier.

Devices detected—This shows the number of devices according to their respective states.

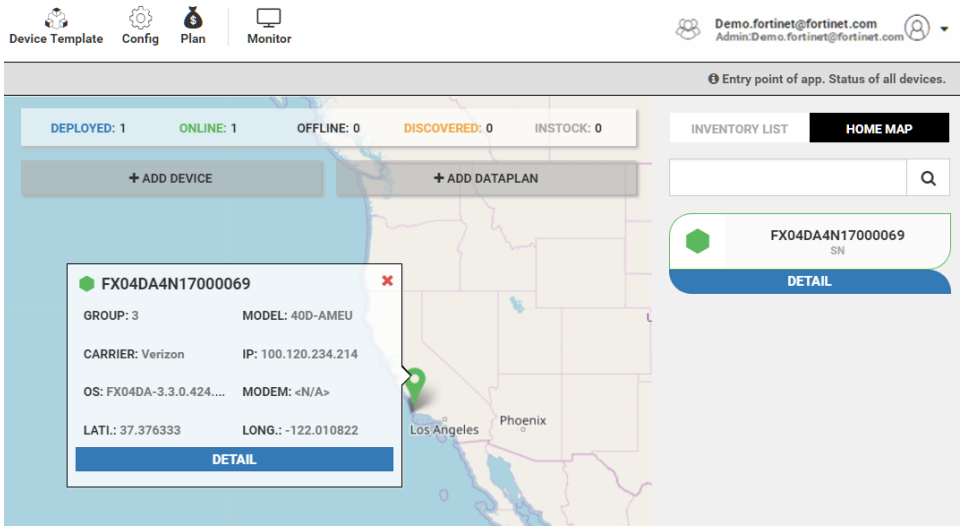
Device management

FortiExtender Cloud gives you the ability to examine details of an individual device and lets you access the device remotely.

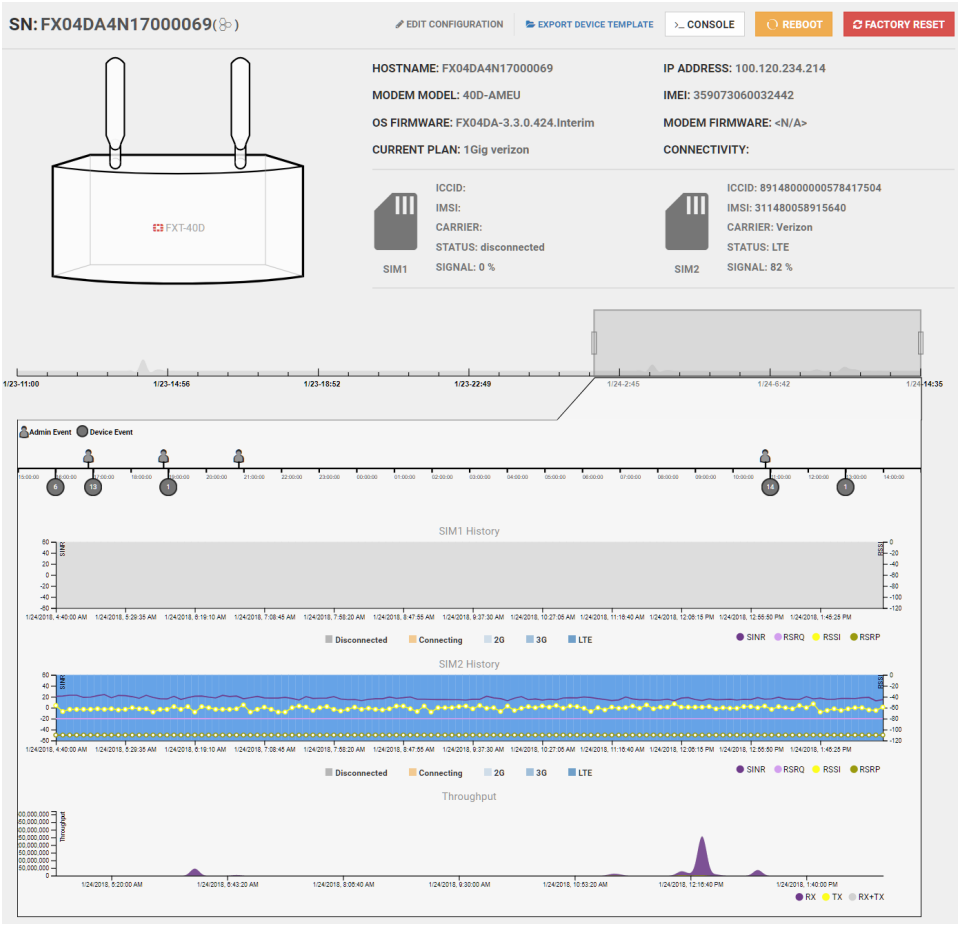
Device details

Viewing device details:

From the Home page, select your device from the list on the right, then click **DETAIL**.



Upon navigating to the device of interest, device specific events, signal statistics and throughput data will appear.



Remote device management

You can manage the selected device using the options at the top of the page.

CONSOLE	Provides CLI access to the device while in the "Deployed" state.
REBOOT	Restarts the device.
FACTORY RESET	Reinitializes the device to factory defaults.

Out of band management

Out of band management (OBM) provides an alternate path to devices at remote locations using FortiExtender's USB to Serial console port adapter.

Using OBM:

1. Enter the following command ito the CLI console:
   ```
   execute obm-console
   ```

2. Select the baudrate of the device being accessed.

Grouping

FortiExtender Cloud gives you the ability to put devices into groups. You can group devices based on department, location, data plan, wireless carrier, or in any other category. Once grouped, devices can be monitored collectively.

A device can be part of multiple groups.

Creating a group

1. Click **Group**, located at the top.
2. Click **ADD NEW GROUP**, then name the group accordingly.

Adding a device to a group

There are two ways to add a device into a group.

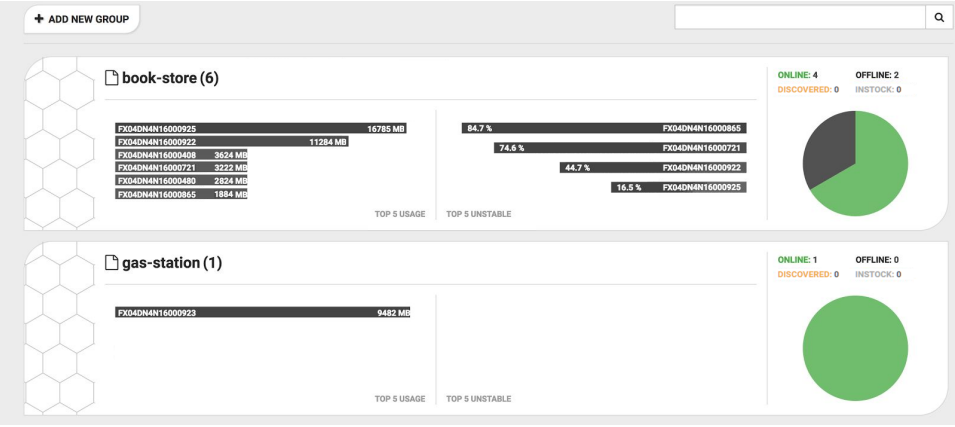
- From the group page, click **ADD DEVICES** accordingly.
- Or, from the Inventory menu, select devices and click **GROUP**.

Removing a group

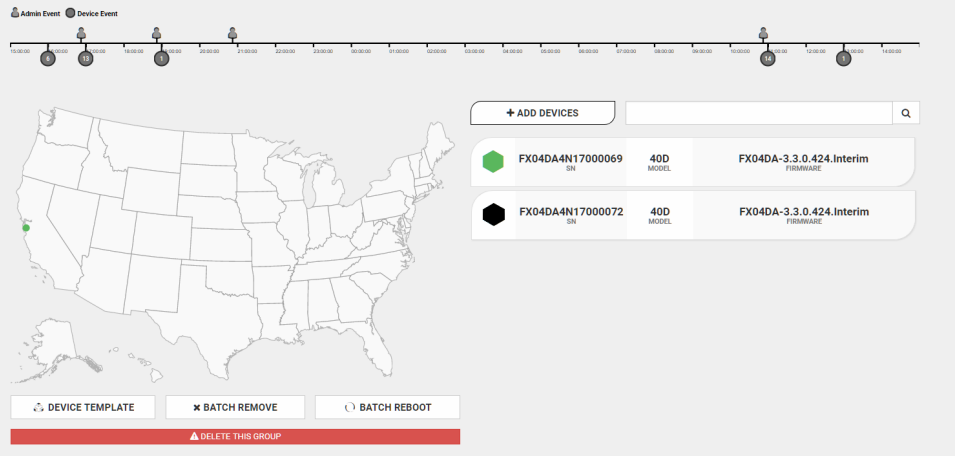
From the group page, click the device group to be removed, then click **DELETE THIS GROUP**.

Monitoring a group

The group page shows data usage, instability, and respective states for devices in the group.



Once the corresponding group is clicked upon, an event line depicting the events and geographic locations of the devices are shown.



Managing within a group

Devices can be rebooted as a batch using the **BATCH REBOOT** button. They can also be removed as a batch using the **BATCH REMOVE** button.

Role Based Access Control

FortiExtender Cloud features Role Based Access Control (RBAC), which allows administrators to add users with either a Viewer role or a (Super) User role.

- Viewers have read only access.
- Users have read-write access.

Using RBAC:

1. Click the Users icon, located at the top right.
   Once in the Users page,the account will display with roles.
2. Click **Add User**.
   A pop-up dialog box will appear.
3. Configure the settings as shown below.

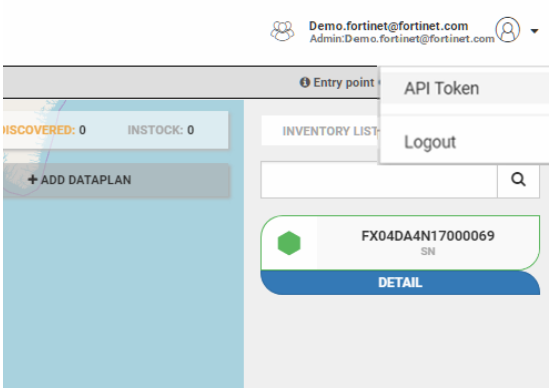
Type	Select Forticare.
User	Enter the Forticare email of the user you wish to add.
Role	Select either Viewer or User.

4. Click **Save**.
   Your new account with corresponding privileges will appear in the list.

API

FortiExtender Cloud provides public APIs. Every FortiExtender Cloud account comes with an API token.

Click on the account name to view the API token.



Keep this token confidential.

How to use the API

Example of a GET call in Python:

```
response = requests.get(url, headers={'Authorization': 'token {}'.format(<your_
    token>)})
```

Example of a POST call in Python:

```
response = request.post(url, headers={'Authorization': 'token {}'.format(<your_
    token>),'content-type': 'application/json'}, data=json.dumps(body))
```

NOTE: Body is in Python object format.

Response status codes:

Code	Description
200	Successful

404	Page not found.
500	Internal server error.

NOTE: If a 500 error occurs, contact the FortiExtender Cloud team.

API commands

Gathering logs

Request:

Protocol: HTTPS

Method: POST

HOST:fortiextender.forticloud.com

URL:/fext/api/public/v1/external/logging/all

Content-Type:application/json

Body:

```
{
   "offset": <integer>
   "size": <integer>
   "sort": {
      <field>: <asc/desc>
      …
   }
   "query": {
      "type": <""|"device_event"|"user"|"fext_stat">
      <field>: <value>
   }
}
```

- offset—The starting position of logs to be retrieved.
- size—The number of logs to be retrieved.
- sort—Sort the logs by given keys such as "@timestamp".
  - field—A key, given as a string.
  - asc/desc—Sort in ascending or descending order.
- query—Filter the logs with fields and values.
  - type—Filter logs by the given log type. If none is given, logs of all types will be returned. There are three log types:
    1. Device_event: The event log generated by the device.
    2. Fext_stat: The device statistics reported by devices.
    3. User: User operation logs with the cloud portal.
  - field—A key, given as a string.
  - value—The value associated with the field given above.

NOTE: You can have multiple fields in query and sort. If you have multiple fields in query, it uses the "and" logic. If you have multiple fields in sort, it will sort in the order of the fields given.

Response:

If successful, it will return the status code 200, as well as the log records which match your filters. If unsuccessful, it will return the status code 500.

```
          {
             "payload" : [
             {
                "system": {
                   "memory": <number>,
                   "sysuptime": <number>,
                   "onlinetime": <number>,
                   "temperature": <number>,
                   "cpu": <number>,
                }
                "modem1": {
                   "plan-name": <string>,
                   "rssi": <number>,
                   "tx": <number>,
                   "rx": <number>,
                   "sinr": <number>,
                   "active-sim": <number>,
                   "rsrq": <number>,
                   "model": <string>,
                   "connection": <string>,
                   "signalstrength": <number>,
                   "latitude": <number>,
                   "longitude": <number>,
                   "IMEI": <string>,
                   "sim1": {
                      "ICCID": <string>,
                      "carrier": <string>,
                      "IMSI": <string>,
                      "connection": <string>,
                   },
                   "sim2": {…}
                }
                "modem2": {…}
                "timestamp": <time>
                "type": <string>
                "sn": <string>
                "ip": <string>
                "host": <string>
             },
             {…},
             …
          ]
       }
```

- SN—Device Serial Number.
- timestamp—The timestamp of this record.

- system—The status of the system.
- modem1—The status of modem one.
- modem2—The status of modem two.
- sim1—The status of SIM card one.
- sim2—the status of SIM card two.

Exporting device information

This API is used to export all device information in an account. The cloud will retrieve all device information from the account associated with the provided API token.

Request:

Protocol: HTTPS

Method: GET

HOST:fortiextender.forticloud.com

URL:/fext/api/public/v1/external/devices/list

Parameters:</?group=<group_name>>

Response:

If successful, it will return the status code 200, as well as the device list. If unsuccessful, it will return the status code 500.

```
      {
         "payload": [
            {
               "sn": <string>,
               "hostname": <string>,
               "state": <string>,
               "model": <string>,
               "firmware": {
                  "current": <string>,
                  "target": <string>,
               },
               "modem_firmware": {
                  "current": <string>,
                  "target": <string>,
               },
               "latitude": <string>,
               "longitude": <string>,
               "opstatus": <string>,
               "groups": [
                  <string>,
                  …
               ]
               "online_status": <string>,
               "sinr": <number>,
               "ip": <string>,
               "imei": <string>,
               "carrier" <string>,
               "lte_config": {
                  "current": {
                     "name": <string>,
                     "version": <number>,
                  },
                  "target": {
                     "name": <string>,
                     "version": <number>,
                  },
               },
            },
            {…},
            …
         ]
   }
```

Export group mapping

This API is used to return the device list of each group selected.

Request:

Protocol: HTTPS

Method: GET

HOST:fortiextender.forticloud.com

URL:/fext/api/public/v1/external/devices/groupmapping

Parameters:</?group=<group_name>>

Response:

If successful, it will return the status code 200, as well as the device lists. If unsuccessful, it will return the status code 500.

```
{
   "payload": {
      "group_name_1": [
         "device_2_sn",
         "device_1_sn",
         …
      ],
      "group_name_2": [
         …
      ],
      …
   }
}
```